

REMARKS

In response to the corrected Final Office Action mailed January 15, 2008 and the Advisory Action mailed April 9, 2008, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks and have added claims. The claims as now presented are believed to be in allowable condition.

Claims 37, 38, and 43-47, 49, and 52 were pending in this Application. By this Amendment, claims 53-54 have been added. Accordingly, claims 37-38, 43-47, 49, and 52-54 are now pending in this Application. Claims 37, 38, 43, 45, 52, and 53 are independent claims.

Rejections under §103

Claims 37, 38, 48 and 50-52 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2003/0226023 (Peters) in view of U.S. Patent No. 6,397,334 (Chainer, et al.). Claims 43-47 and 49 were rejected under 35 U.S.C. §103(a) as being unpatentable over Peters in view of Chainer and further in view of U.S. Patent No. 5,517,568 (Grube, et al.).

Applicants respectfully traverse these rejections and request reconsideration. The claims are in allowable condition.

Peters teaches a technique for deterring theft of media recording devices (Abstract). A media file recorded by a recording device is encrypted, so that it cannot be properly played back without a cryptographic key supplied to the owner of the device (Paragraph 0023). Because asymmetric public key encryption is more secure but also more complex (and therefore slower) than symmetric shared key encryption, a symmetric key may be used to encrypt the media files while the symmetric key is encrypted using public key encryption. (Paragraph 0031). In order to aid a customer who has lost his or her key to a device, a manufacturer may provide a key escrow service to give a customer the

key upon presentation of some proof of ownership of the device (Paragraph 0043).

Chainer discloses a system and method for authenticating an image of an object (Abstract). An object 102 contains one or more tags 101, such as RFID tags, which are not functionally removable from the object 102 (Col. 3, line 63 through Col. 4, line 8). A tag reader 103 (such as an RFID tag reader) reads the RFID tags 101 as a coupled camera system 104 records an image of the object 102 (Col. 4, lines 27-36). A composite generator 105 combines the image and the sensed RFID results to encode the tag ID information together with a hash of the image (Col. 4, lines 37-48). This encoded data may be encrypted for further security (Col. 5, lines 43-54). In addition, other measuring devices 400 may record additional properties of an object 406 in order to provide additional information with which to identify an object (Col. 6, lines 17-38). In addition, a zoom lens 108 may be used to take multiple pictures of an object 102 with different settings (Col. 6, lines 39-45).

Grube discloses a method for detecting unauthorized use of a communication unit 102 in a secure wireless communications system 100 (Col 2, lines 44-45). If a communication unit 102 sends an encrypted communication encrypted with inactive, previously used, encryption parameters (such as a inactive encryption key), then this is detected by system manager 110 (Col. 3, lines 21-36), and the communication unit 102 is flagged as an unauthorized unit (Col. 4, lines 48-60).

Applicants point out that the Advisory Action mailed April 9, 2008 did not respond to all of Applicants' arguments as presented in Applicants' previous Amendment, dated March 17, 2008. Applicants respectfully request that the arguments presented in that previous response be fully considered and responded to in the next Office Action.

Claims 43 and 44

Claim 43 (which has now been placed into independent form by incorporating all the limitations previously found in canceled base claim 17) recites a method for generating an output signal from a video data acquisition system. The method includes (a) receiving a video signal that varies depending on sensed images, (b) encrypting the video signal using a first key, (c) encrypting the first key using a second key, (d) including at least the encrypted first key and encrypted video signal in the output signal, (e) implementing a recognition algorithm to identify objects associated with the sensed images, (f) in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal, and (g) randomly generating a new encryption key for encrypting different portions of the video signal over time. Implementing the recognition algorithm to identify objects associated with the sensed images includes analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.

The Advisory Action did not respond to several of Applicants' arguments presented in the Amendment dated March 17, 2008. In particular, Applicants argued, on page 12, that Chainer does not teach *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal*, because any identity verification takes place subsequent to recording the additional data. Applicants hereby fully incorporate that argument herein by reference. Applicants respectfully request that this argument be fully considered and responded to in the next Office Action.

In addition, Applicants argued, on pages 12-13, that Grube does not teach *randomly generating a new encryption key*. Applicants hereby fully incorporate that argument herein by reference. Applicants respectfully request that this argument be fully considered and responded to in the next Office Action.

-12-

In addition, with respect to claim 44, Applicants argued, on page 14, that Chainer does not teach *encrypting data identifying objects* associated with the sensed images *with a third key, the third key being distinct from the first key*. Applicants hereby fully incorporate that argument herein by reference. Applicants respectfully request that this argument be fully considered and responded to in the next Office Action.

Claims 37-38, 45-47, 49, and 52

Applicants argued, on pages 14-17 of the Amendment dated March 17, 2008, that claims 37-38, 45-47, 49, and 52 recite limitations similar to those found in claims 43 and 44 and accordingly distinguish over the prior art for similar reasons. Applicants hereby fully incorporate those arguments herein by reference. Applicants respectfully request that those arguments be fully considered and responded to in the next Office Action.

Newly Added Claims

Claims 53-54 have been added and are believed to be in allowable condition. Claim 53 is independent, and claim 54 depends from claim 53. Support for claim 53 is provided within the Specification, for example, on page 13, line 28 through page 17, line 28. Support for claim 54 is provided within the Specification, for example, on page 18, line 3 through page 19, line 7.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after this Amendment, that the Application is not in condition for

-13-

allowance, the Examiner is respectfully requested to call the Applicants' Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Amendment, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Michael Ari Behar/

M. Ari Behar, Esq.
Attorney for Applicants
Registration No.: 58,203
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1004-120

Dated: April 15, 2008